Forgery Detection on an Image Copy-Move

Vuthukota Divya

Dept of Computer Science , SV University, Tirupati

***Abstract*—** *Copy-move forgery is one of the most commonly used manipulations for tampering digital images. Key point-based detection methods have been reported to be very effective in revealing copy-move evidence due to their robustness against various attacks, such as large-scale geometric transformations. However, these methods fail to handle the cases when copy-move forgeries only involve small or smooth regions, where the number of key points is very limited. To tackle this challenge, we propose a fast and effective copy-move forgery detection algorithm through hierarchical feature point matching. We first show that it is possible to generate a sufficient number of key points that exist even in small or smooth regions by lowering the contrast threshold and rescaling the input image. We then develop a novel hierarchical matching strategy to solve the key point matching problems over a massive number of key points. To reduce the false alarm rate and accurately localize the tampered regions, we further propose a novel iterative localization technique by exploiting the robustness properties (including the dominant orientation and the Scale information) and the color information of each key point. Extensive experimental results are provided to demonstrate the superior performance of our proposed scheme in terms of both efficiency and accuracy.*

I. INTRODUCTION

The development of modern image editing software's, such as Photoshop and Gimp, digital images can be forged at a very low cost. This brings a big threat for the reliability of digital images. Copy-move forgery is one common manipulation among various digital image forgeries, where one or several regions of an image are pasted elsewhere in the same image in order to hide or duplicate objects of interest. Such process may be accompanied with rotation, resizing, compression and noise addition to make the final forgeries more convincing. Detecting them sometimes can be very challenging, especially when the copy-move forgery only involves small or smooth regions, or when the forged areas have been processed by some severe attacks, such as large-scale resizing and heavy noise addition. Where the copy-move forgeries are conducted over only smooth or small regions. In the recent years, many image copy-move forgery detection methods have been proposed, which can be roughly categorized into two groups: 1) dense-field (or block-based) approaches and 2) sparse-field (or key point-based) approaches. For the dense-field copy-move forgery detection approaches, the input images are first divided into overlapped and regular blocks; then the forgery localization procedure is performed through block matching. The dense-field approaches were shown to be more accurate than the key point-based ones at the cost of higher complexity. More recently, proposed an efficient dense-field copy move forgery detection method, where the processing time was highly reduced by resorting to the Patch Match algorithm a fast approximate nearest-neighbor search scheme. Unfortunately, all the existing dense-field schemes suffer from some attacks, such as scaling, rotation and noise addition. For brevity, we call such key point-based techniques involving clustering procedures as *key point-clustering-based* algorithms. Instead of using the clustering algorithms to group the matched key points, some other researchers proposed to first segment the whole image into non-overlapped small patches; the matching process was then conducted between each two segmented regions . In our work, we call those key point-based techniques involving segmentation procedures as *key point-segmentation-based* algorithms. Besides the SIFT descriptor, were also considered in the recent literatures. Though the key point-based copy-move forgery detection methods have been studied from various aspects, they were unfortunately shown to be less accurate than the dense-field ones , and the performance gap was quite large when the copy-move forgery only involves small or smooth regions as shown in Fig. 1. The main drawbacks of the existing key point-based copy-move forgery detection methods can be summarized as follows:

1) They fail to generate a sufficient number of key points (hence matched pairs) in those small or smooth copy move regions, causing detection failure;

2) It is very difficult (even impossible) to find a *universally good* clustering/segmentation algorithm and associated parameters applicable for all images. This is because the copy-move regions can be of any sizes, and can be highly diverse from the textures. In addition, the number of copy-move regions is typically unknown; properly performing the clustering in this case is difficult;

3) The existing key point-based methods lack of reliable affine matrix validation and inliers selection, in the sense that some outliers could be treated as inliers by the existing holography estimation techniques (e.g., RANSAC), causing a high false alarm rate. In this paper, we propose an efficient and accurate key point-based method for image copy-move forgery detection and localization, achieving consistently good performance even if the copy-move forgery only involves smooth or small regions, or the forged images have been processed by some. severe attacks (e.g., large-scale resizing and heavy noise addition presents the framework of our proposed image forgery detection scheme, which follows the classic workflow, namely, 1) feature extraction; 2) feature matching; and 3) forgery localization. Our main contribution lies in designing novel and sophisticated solutions for *all* these three steps. At the first stage, we design a simple yet effective way to extract a sufficient number of SIFT key points, even in smooth and small regions, by lowering the *contrast threshold* and rescaling the input image. At the second stage, a novel hierarchical point matching strategy is proposed to solve the *key point matching problems* over a massive number of key points. At the third stage, a novel iterative holography estimation and a copy-move localization technique are suggested, without involving any clustering and segmentation procedures. By fully exploiting the robustness properties (including the dominant orientation and the scale information) and the color information of each key point, our proposed method achieves very accurate detection results at considerably lowered computational cost. Extensive experimental results demonstrate that our proposed scheme leads to a higher True Positive Rate (TPR) and a lower False Positive Rate (FPR) simultaneously in most of the cases, compared with both the existing dense-field and key point-based approaches. *Difference from the Conference Version:* Portions of the work presented in this paper have previously appeared in as a conference version. We have substantially refined the paper in terms of both technical and experimental parts. The primary improvements can be summarized as follows. First of all, we carefully present the strategy to select inliers

II. PROPOSED WORK

We have proposed a fast and effective key point-based copy-move forgery detection and localization technique. By carefully studying the key point extraction algorithm (SIFT), we have first demonstrated that it is possible to generate a sufficient number of key points even in

smooth or small regions, by lowering the contrast threshold and resizing the image. The detection performance is measured at both the image level and the pixel level. At the image level, we focus on the ability that an image can be correctly recognized as forged or genuine; at the pixel level, we analyze the performance for forgery localization accuracy.

Advantages:

- The matching procedure is of very low computational and effective to alleviate the critical matching problems.
- A large number of matches are found by resorting to the scale clustering strategy, showing its effectiveness to migrate the key point matching problem.
- It can be readily figured out that the computational cost is significantly reduced by the overlapped gray level clustering
- The relatively low computational cost of running individual.

III. METHODOLOGY

3.1 Input image

Import two images' files one is normal image another one is tempered image of that original image.

3.2 Pre-processing

In pre-processing we firstly resize the original image then we enhanced that image towards contrast and remove noise using Gaussian filter.

3.3 Feature matching using sift

The SIFT algorithm can be roughly divided into four phases:

i) candidate keypoint identification through the scale space extrema detection;

ii) key points refinement according to the contrast and edge thresholds;

iii) dominant orientation assignment of each keypoint; and

iv) feature descriptor generation.

3.4 Scale Space Extrema Detection

At phase i), the candidate key points are identified at different scales. Given an input image **I**, successive Gaussian-blurred images are generated by repeatedly convolving **I** with Gaussian filters at multiple scales. Then, the candidate SIFT key points are selected as local extrema. At phase ii), all the candidate key points are further refined according to a contrast threshold and an edge threshold. This procedure plays a key role for rejecting unstable extrema in the SIFT algorithm.

At phase iii), a dominant orientation is assigned to each survived keypoint to achieve rotation invariance. An orientation histogram is then constructed by gathering the gradient orientation information of points in a local window centered at the SIFT keypoint. The peak in the orientation histogram corresponds to the dominant orientation. At phase iv), a 128-dimensional descriptor is calculated by encoding the surrounding information in a local area centered at the SIFT keypoint.

3.5 SIFT Feature Matching

To find a reliable match (may not exist though) of the keypoint **k**, simply evaluating the distances with the other (n −1) key points against a global threshold does not perform well in the high dimensional feature space. The

Widely used matching algorithm was suggested in the original SIFT, where the matching procedure is conducted by evaluating the ratio of the closest distance to the second closest one. The rationale behind is that for those false matches, there will very likely be several other false matches with similar distances. This is because the distances are computed.

3.6 Key point Descriptor

Now keypoint descriptor is created. A 16x16 neighbourhood around the keypoint is taken. It is divided into 16 sub-blocks of 4x4 sizes. For each sub-block, 8 bin orientation histogram is created. So a total of 128 bin values are available. It is represented as a vector to form keypoint descriptor. In addition to this, several measures are taken to achieve robustness against illumination changes, rotation etc

3.6.1 Keypoint Matching

Key points between two images are matched by identifying their nearest neighbours. But in some cases, the second closest-match may be very near to the first. It may happen due to noise or some other reasons. In that case, ratio of closest-distance to second-closest distance is taken.

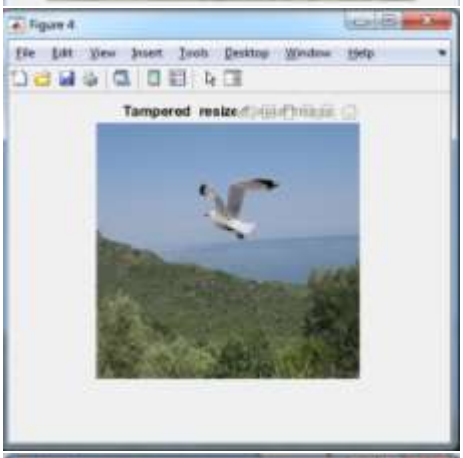
3.7 Copy detection

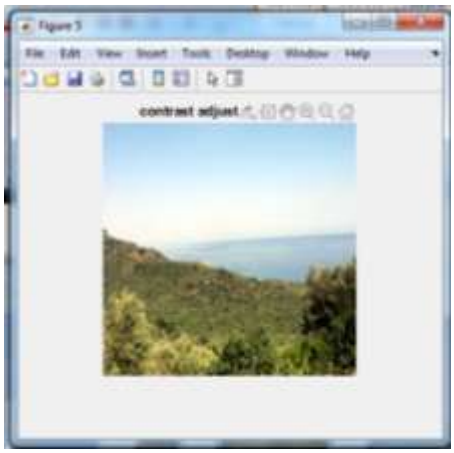
The capability of our proposed method against the extremely smooth copy-move forgery gives an example where the copy-move forgery only involves smooth regions (the variance of the copied region). In order to generate extremely smooth copy-move forgeries, we continuously smooth the copy-move regions using Gaussian filters with STD varying from 2 to 7. Finally, we obtain a set of copy-move images with variances of the copied regions gradually changing from 26.10 to 0.38. it draws the pixel level F1 curves for different algorithms over the Generated images. Note that the image is successfully detected as a forgery when the F-pixel is bigger than 0. As can be seen, our method is able to detect the forgery with high localization accuracy even when the variance of the copied region is about 1, in which case the copy-move areas are extremely smooth (the average offset from the mean is only about 1).

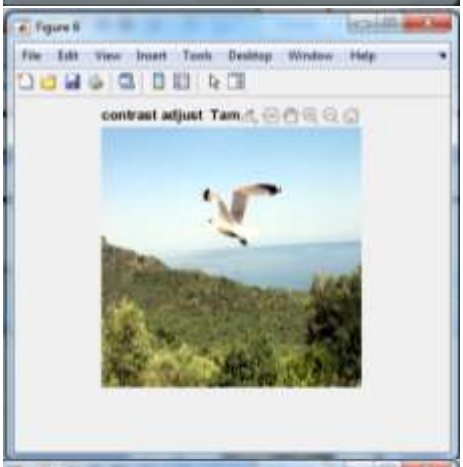
3.8 Localization

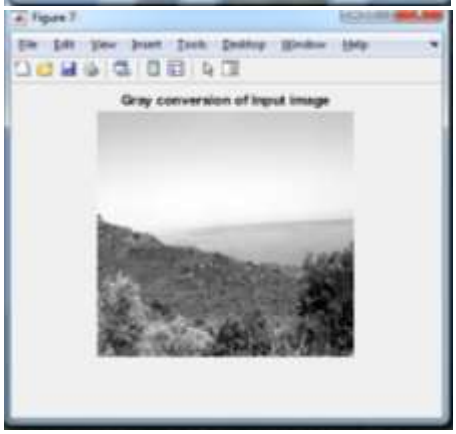
The forgery localization in dense fields can be simply conducted by merging the neighboring segmented regions containing a sufficient number of matched key points. However, as aforementioned, it is practically challenging to find a universally good segmentation algorithm and the associated parameters applicable for all images. Below we propose a new algorithm for the forgery localization in dense fields, without involving any troublesome clustering/segmentation procedures. Specifically, our method is composed of two phases: 1) construct the suspicious regions according to the scale information of each inlier; and 2) refine the suspicious regions by validating the consistency of the color information.

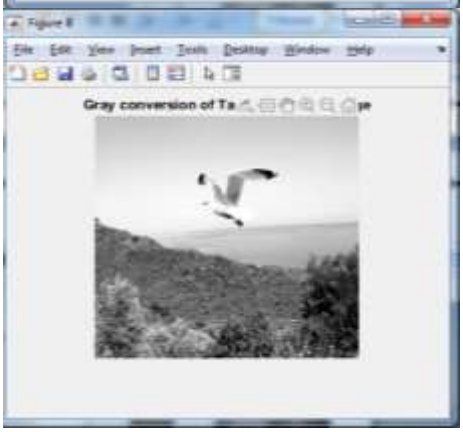
IV. IMPLEMENTATION

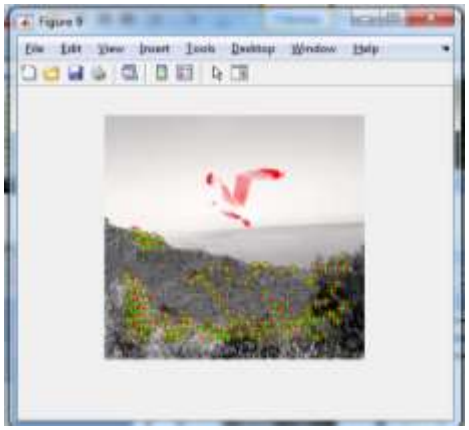


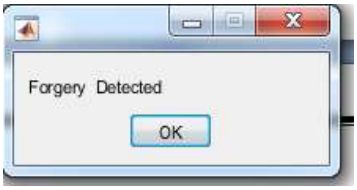


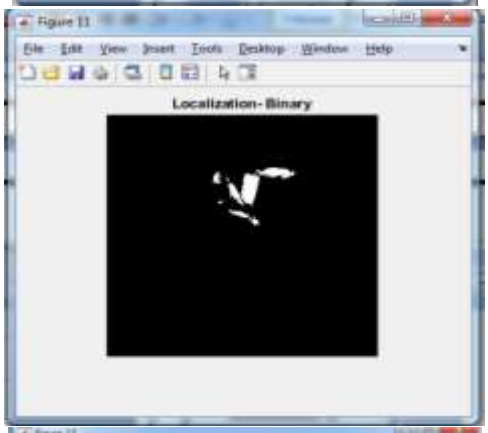


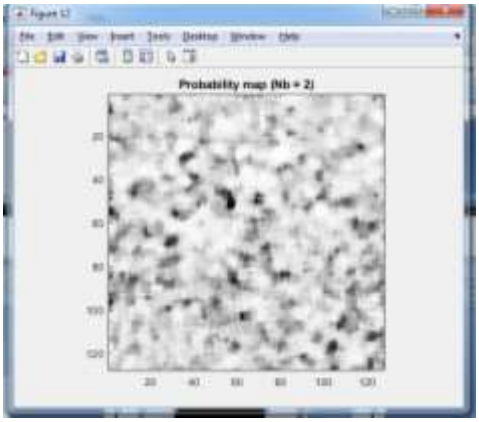


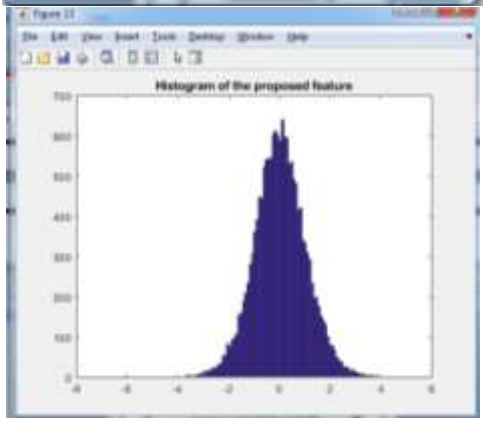












V. CONCLUSION

In this paper, we have proposed a fast and effective key point-based copy-move forgery detection and localization technique. By carefully studying the key point extraction algorithm (SIFT), we have first demonstrated that it is possible to generate a sufficient number of key points even in smooth or small regions, by lowering the contrast threshold and resizing the image. Then a novel hierarchical feature point matching strategy has been proposed to alleviate the critical matching problems. To reduce the false alarm rate and accurately localize the copied regions, we have further proposed a novel iterative localization scheme without involving any clustering and segmentation procedures. By fully exploiting the robustness properties of the SIFT algorithm (including the dominant orientation and the scale information) and the color information of each key point, our proposed technique achieves very high detection accuracy. Extensive experimental results have been provided to demonstrate the superior performance of our proposed scheme.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, 2003, pp. 10.

[2] G. Muhammada, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digit.Invest., vol. 9, no. 1, pp. 49–57, 2012.

[3] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[4] Y. Li, J. Zhou, A. Cheng, X. Liu, and Y. Y. Tang, "SIFT keypoint Removal and injection via convex relaxation," IEEE Trans. Inf. Forensics Security, vol. 11, no. 8, pp. 1722–1735, Aug. 2016.

[5] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy move forgery detection scheme," IEEE Trans. Inf. Forensics Security,vol. 10, no. 3, pp. 507–518, Mar. 2015.

[6] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[7] Y. Li, J. Zhou, and A. Cheng, "SIFT keypoint removal via directed graph construction for color images," IEEE Trans. Inf. Forensics Security,vol. 12, no. 12, pp. 2971–2985, Dec. 2017.

[8] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, NH, USA,Tech. Rep. TR2004-515, 2004.

[9] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Sci. Int., vol. 233, nos. 1–3, pp. 158–166, 2013.

[10] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 1053–1056.